

RECEIVED SEP 10 1950

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT WE, Shinkichi Gama, a citizen of Japan residing at Yokohama-shi, Kanagawa, Japan and Shogo Shibazaki, a citizen of Japan residing at Yokohama-shi, Kanagawa, Japan have invented certain new and useful improvements in

Sub
a1
a1 / ~~STORAGE DEVICE~~

of which the following is a specification : -

TITLE OF THE INVENTION

~~STORAGE DEVICE~~

a1 >

BACKGROUND OF THE INVENTION

5 1. Field of the Invention

The present invention generally relates to storage devices including non-volatile memory that maintain data after a power source is shut off, and more particularly to a storage device that can
10 execute a test process based on a test signal output from a test terminal while maintaining high security.

It is important to maintain high security for data stored in the storage device. It is also important to improve the quality of the storage
15 device.

To improve the quality of the storage device, it is required to test for failures in storage devices after assembly is completed. Generally, it is needed to provide a test terminal to
20 test the storage device. However, the provided test terminal makes it possible for outsiders to easily obtain data such as a cipher key or secret data stored in the storage device.

Consequently, it is desired to not only
25 realize higher security but also develop a technology to test fully assembled storage devices.

2. Description of the Related Art

For example, a non-volatile storage device such as a memory stick is used to record an encrypted
30 copyrighted product such as music.

In a case in which the test terminal is provided for the storage device, when the cipher key is read by an illegal user, the copyrighted product may be easily pirated.

35 Further, an authentication is processed based on cipher text by using a shared cipher key between the non-volatile memory and a host device for

Sub
a1

00534105-0347000

Disadvantageously, in this case, when the cipher key is read, a host device used by the illegal user can obtain data from the non-volatile memory by
5 utilizing the test terminal.

In the above conventional non-volatile memory, illegal users' infringement can be prevented and high security can be maintained.

In the conventional manner, it is difficult to improve the quality of the non-volatile
20 memory.

It is a general object of the present invention to provide a storage device maintaining data when the power source is shut off, which can execute a test process based on test signals by using a test terminal while maintaining high security, in which the above-mentioned problems are eliminated.

The above first object of the present invention is achieved by a storage device for

35 According to the present invention, when
the secret data is stored, the test process is
prohibited by cutting off the test signals.

The above first object of the present invention is achieved by a storage device for maintaining information when power is OFF and being capable of executing a test process based on test signals, including: a maintaining part maintaining, in a volatile state, information indicating that an access request is conducted to a memory storing secret data; and a cutting-off part cutting off the test signals input from a test terminal when the maintaining part maintains the information indicating that the access request is conducted to the memory storing secret data.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG.1 is a diagram showing a principle configuration of a storage device according to a first embodiment of the present invention;

FIG.3 is a schematic diagram showing an
35 operation between a host device and a storage device
controller according to the present invention;

FIG.4 is a diagram showing a security part

according to the first embodiment of the present invention;

FIG.5 is a diagram showing a sequencer of the security part according to the first embodiment of the present invention;

FIG.6 is a diagram showing a security part according to a second embodiment of the present invention;

FIG.7 is a diagram showing a security part according to a third embodiment of the present invention;

FIG.8 is a diagram showing a configuration of a sequencer according to the third embodiment of the present invention;

FIG.9 is a diagram showing a security part according to a fourth embodiment of the present invention; and

FIG.10A is a flow chart for explaining a process of the storage device controller in the configuration in FIG.4 according to the first embodiment of the present invention and FIG.10B is a flow chart for explaining a process of the storage device controller in the configuration in FIG.7 according to the first embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG.1 is a diagram showing a principle configuration of a storage device according to a first embodiment of the present invention.

FIG.1 shows a storage device 1 according to the present invention that can maintain data when the power source is shut off and execute a test process based on a test signal input from a test terminal.

The storage device 1 according to the present invention includes a secret data storing part

10, circuit parts 11-i ($i = 1$ through n), a test input I/F (interface) part 12, a cutting-off part 13, an instruction part 14, a decoding part 15 and a maintaining part 16.

5 The secret data storing part 10 stores secret data including cipher keys. When there is no secret data to be stored, data that is different from any secret data is stored as initial data. When
10 secret data is stored and a data area other than the secret data area storing the secret data is provided, the secret data storing part 10 may store data indicating a presence of secret data in the other data area.

 The circuit parts 11-i ($i = 1$ through n)
15 read the secret data from the secret data storing part 10 and execute a predetermined process by using the secret data. The test input I/F part 12 sends test signals, which are received from a test terminal, to the circuit parts 11-i via the cutting-off part 13.
20 The cutting-off part 13 cuts off test signals from the test input I/F part 12.

 The instruction part 14 sends a data reading instruction to the secret data storing part 10. The decoding part 15 determines by decoding data
25 read from the secret data storeing part 10 whether or not the secret data is stored. The maintaining part 16 maintains in a volatile state a decryption result produced by the decoding part 15.

 In the storage device 1 configured above,
30 the instruction part 14 sends a data reading instruction to the secret data storing part 10 to read normal data when the power source is turned ON or when the storage device is reset or when a command for processing secret data is received.

35 At the same time, the instruction part 14 sends the secret data storing part 10 a data reading instruction to read the secret data, to read data

0054405-034700

5

10

15

20

30

35

When the encrypting/decrypting circuit 570 receives the random number from the random number generating circuit 571, the encrypting/decrypting circuit 570 reads one cipher key indicated by the random number from the cipher key storage area of the controller memory 56 and encrypts the read cipher key by using the random number provided and then sends the encrypted cipher key as cipher text to the host device 30.

When receiving the cipher text from the
20 host device 30, the encrypting/decrypting circuit 570
decrypts the cipher text by using the same cipher key.

In order to ensure the quality of the storage device 20 having the storage device

controller 50 capable of processing as mentioned above, it is required to test whether or not the storage device controller 50 performs as designed. However, if the storage device controller 50 can
5 perform this function, it is possible for an illegal user to steal the cipher keys by utilizing the function.

Thus, in order to eliminate this disadvantage, the security part 58 is provided in the
10 storage device controller 50 as shown in FIG.2.

FIG.4 is a diagram showing the security part 58 according to the first embodiment of the present invention. In FIG. 4, parts that are the same as those shown in FIG.2 or FIG.3 are given the
15 same reference numbers.

In FIG.4, the security part 58 includes a sequencer 580, a test input interface 581, a test selecting part 582, an output part 583, a register 584, a decoder 585 and a control flag latching
20 circuit 586.

The sequencer 580 is executed by power ON and executes an entire process. The test input interface 581 conducts test signals input from the test terminal and decodes the test signals so as to
25 execute a test function corresponding to the test signals.

The test selecting part 582 determines to cut off test signals output from the test input interface 581 based on a control flag latched by the
30 control flag latching circuit 586. The output part 583 outputs the test signals to the test output terminal.

The register 584 maintains data retrieved from the controller memory 56. The data is the
35 cipher key when the cipher key is stored or the initial data when the cipher key is not stored.

The decoder 585 determines whether or not

the data stored in the register 584 is the cipher key, by decoding the data stored in the register 584. The control flag latching circuit 586 controls the test selecting part 582 by latching a result decoded from the decoder 585.

FIG.5 is a diagram showing a sequencer of the security part according to the first embodiment of the present invention.

As shown in FIG.5, the sequencer 580 includes a sequencer operation flag ON part 5800, a sequence counter 5801, a sequencer end-signal generating part 5802, a memory address generating part 5803, a read-signal generating part 5804 and a register store-signal generating part 5805.

The sequencer operation flag ON part 5800 turns ON an operation flag when power is turned ON. The sequence counter 5801 increments a counter while the operation flag is ON. When the counter reaches a predetermined value, the sequence counter 5801 executes the memory address generating part 5803, the read-signal generating part 5804 and the register store-signal generating part 5805. The sequencer end-signal generating part 5802 generates an end-signal to turn OFF the operation flag when the counter of the sequence counter 5801 reaches a maximum value.

The memory address generating part 5803 generates a memory address indicating the cipher key stored in the controller memory 56. The read-signal generating part 5804 generates a read-signal indicating to read data from the controller memory 56. The register store-signal generating part 5805 generates a register store-signal as a timing signal to store in the register 584.

The security part 58 configured as described above can prevent information stored in the storage device 20 from being read by illegal users.

That is, the sequencer 580 provided in the security part 58 starts the sequence counter 5801 to count when power is turned ON. The sequence counter 5801 executes the memory address generating part 5803 to generate a memory address indicating the cipher key in the controller memory 56. Subsequently, the read-signal generating part 5804 is executed to generate a read-signal indicating to read data from the controller memory 56.

10 In response to the generated memory address and read-signal, the controller memory 56 reads data, for example, 16 bytes of data from the indicated memory address. That is, the cipher key is read when the cipher key is stored or the initial data is read when the cipher key is not stored.

Thereafter, the sequencer 580 generates a register store-signal to be a store-timing signal for the register 584 by executing the register store-signal generating part 5805.

20 In response to the register store-signal, the register 584 maintains the data read from the controller memory 56.

As mentioned, when the data read from the controller memory 56 is stored in the register 584, the decoder 585 decodes the data so as to determine whether the data is the cipher key or the initial data. Based on the result of the decoder 585, for example, the control flag latching circuit 586 latches "1" into the control flag when the data maintained in the register 584 is the cipher key or "0" into the control flag when the data maintained in the register 584 is the initial data.

Based on the control flag latched by the control flag latching circuit 586, the test selecting part 582 cuts off the test signal output from the test input I/F part 581 to prevent executing the test function when the data maintained by the register 584

is the cipher key. On the other hand, the test selecting part 582 does not cut off the test signals but carries out the test function when the data maintained by the register 584 is the initial data.

5 In this method, the security part 58 prohibits transferring to a test mode when the cipher key is stored in the controller memory 56 when power is ON. Therefore, it is possible to prevent the reading of the cipher keys by utilizing the test
10 function.

Moreover, the security part 58 controls transfer to the test mode when any cipher key is not stored in the controller memory 56 when power is ON. Therefore, it is possible to test to check whether or
15 not the storage device controller 50 is performs as designed.

That is, when the storage device controller 50 is tested, a maker of the storage device 20 uses the host device 30 to delete the
20 cipher keys stored in the controller memory 56 (reset the controller memory 56) and turns off and on the power. Consequently, the test mode becomes available.

The security part 58 carries out the same method when the controller memory 56 is reset. Since
25 the cipher keys are deleted by the reset, the test signals output from the test input I/F part 581 are not cut off and then the test function is executed.

When a user maker, which stores information into the storage device 20 to sell the
30 information, requires a specific address for the cipher keys, the maker of the storage device 20 designs the memory address generating part 5803 such that the memory address generates the specific address for the cipher keys.

35 However, when the user maker does not require such a specific address, the storage device maker designs the storage device 20 such that the

ORIGINAL SOURCE

memory 56. Based on the result, the control flag latching circuit 586 latches the control flag. In addition, when the controller memory 56 is reset, it is determined whether or not the cipher keys are stored in the controller memory 56. Based on the result, the control flag latching circuit 586 latches the control flag. Further, the same process may be carried out at other times.

FIG.6 is a diagram showing a security part according to a second embodiment of the present invention. In FIG.6, parts that are the same as those shown in the previously described figures are given the same reference numbers and the explanation thereof will be omitted.

For example, as shown in FIG.6, a command interpreting part 587 is provided in the security part 58 to interpret a command. When the command interpreting part 587 detects a command for processing the cipher keys, the command interpreting part 587 determines whether or not the cipher keys are stored in the controller memory 56. Based on the determination result, the control flag latching circuit 586 latches the control flag.

FIG.7 is a diagram showing a security part according to a third embodiment of the present invention. In FIG.7, parts that are the same as those shown in the previously described figures are given the same reference numbers and the explanation thereof will be omitted.

In the first embodiment described in FIG.4, in a case in which the cipher keys are stored in the controller memory 56 when the power source is ON, since it is prohibited to transfer in the test mode, it is possible to prevent information stored in the storage device 20 from being read by illegal users. In the third embodiment in FIG.7, when the encrypting/decrypting circuit 570 reads the cipher

"1", which indicates that the data maintained in the register 584 is the cipher key, into the control flag.

Based on the control flag latched by the control flag latching circuit 586, the test selecting part 582 cuts off the test signals output from the test input I/F part 581 to prohibit from executing the test function.

In this approach, the security part 58 cancels a current working test process in the test mode or prohibits transferring from the normal mode to the test mode. Therefore, it is possible to be certain of preventing information including the cipher keys stored in the storage device 20 from being read illegally by utilizing the test function.

In the third embodiment in FIG.7, by maintaining the cipher key read from the encrypting/decrypting circuit 570 in the register 584, the control flag latching circuit 586 latches the control flag to cut off the test signals. But alternatively, as shown in FIG.9, which is a diagram showing a security part according to a fourth embodiment of the present invention, in response to the access signal output from the encrypting/decrypting circuit 570, the sequencer 580 controls the control flag latching circuit 586 to latch the control flag in order to cut off the test signals.

FIG.10A is a flow chart for explaining a process of the storage device controller in the configuration in FIG.4 according to the first embodiment of the present invention.

In FIG.10A, when the power source is turned on, the storage device controller 50 reads data from the cipher key storage area of the controller memory 56 (step ST1). When the read data does not indicate the reset data, that is, when the read data is the cipher key, the test signals are cut

off and the test process is prohibited (steps ST2 and ST3). On the other hand, when the read data is reset data, it is allowed to input test signals and the test process is executed (step ST4).

5 In this configuration of the storage device 20, it is prohibited to transfer to the test mode when the cipher keys are stored in the controller memory 56. Therefore, it is possible to be certain to prevent the cipher keys stored in the
10 storage device 20 from being read illegally by utilizing the test function.

FIG.10B is a flow chart for explaining a process of the storage device controller in the configuration in FIG.7 according to the first
15 embodiment of the present invention.

In FIG.10B, when the encrypting/decrypting circuit 570 outputs the access request to access the cipher keys, the storage device controller 50 cuts off the test signals. Thus, the test process can be
20 prohibited or a working test process can be canceled.

In this configuration of the storage device 20, when the cipher key is read from the controller memory 56, it is possible to prevent transferring to the test mode or to immediately
25 cancel the test mode. Therefore, it is possible to be certain in preventing the cipher keys stored in the storage device 20 from being read illegally by utilizing the test function.

The embodiments described above are not
30 limited to protect the cipher keys only.

The present invention is not limited to the specifically disclosed embodiments, variations and modifications, and other variations and modifications may be made without departing from the
35 scope of the present invention.

The present application is based on Japanese Priority Application No. 11-195527 filed on

0052405:034700

[illegible]